WE CLAIM:

1. A system for increasing the security and efficiency of cryptographic processing resources for postal franking machines, comprising:

(a) an encryption engine;

(b) means for obtaining encrypted code in portions to be processed by the encryption engine;

(c) random access memory;

(d) means for placing decrypted output from the encryption engine into the random access memory.

2. A method for increasing the security and efficiency of cryptographic processing resources for postal franking machines, comprising:

(a) obtaining encrypted code in portions to be processed by an encryption engine;

(b) placing decrypted output from the encryption engine into random access memory.

3. A system for protecting cryptographic processing and memory resources for postal franking machines, comprising:

(a) (1) zeroizing circuitry, (2) read only memory, (3) random access memory, (4) a clock circuit, (5) non-volatile memory, (6) central cryptographic processor, (7) logic for addressing and data flow, (8)

crypto key retention, (9) signature algorithm execution, (10) random number generator, (11) interrupt control and porting, (12) real time calendar clocking and watch-dog timer, (13) hash algorithm, (14) secure memory management unit, and (15) host interface, all disposed within a PCMCIA Card;

(b) means disposed within the PCMCIA Card for monitoring the amount of time a host controller is taking to complete a bus transaction;

(c) means disposed within the PCMCIA Card for comparing the monitored amount of time to a predetermined reference time;

(d) means disposed within the PCMCIA Card for refusing to permit completion of the bus transaction if the monitored amount of time exceeds the predetermined reference time;

(e) an encryption engine disposed within the PCMCIA Card;

(f) means for obtaining encrypted code in portions to be processed by the encryption engine;

(g) random access memory disposed within the PCMCIA Card;

(h) means for placing decrypted output from the encryption engine into the random access memory.

4. A system for protecting cryptographic processing and memory resources for postal franking machines, comprising:

(a) (1) zeroizing circuitry, (2) read only memory, (3) random access memory, (4) a clock circuit, (5) non-volatile memory, (6) central cryptographic processor, (7) logic for addressing and data flow, (8) crypto key retention, (9) signature algorithm execution, (10) random number generator, (11) interrupt control and porting, (12) real time calendar clocking and watch-dog timer, (13) hash algorithm, (14) secure memory management unit, and (15) host interface, all disposed within a PCMCIA Card;

(b) means disposed within the PCMCIA Card for monitoring the amount of time a host controller is taking to complete a bus transaction;

(c) means disposed within the PCMCIA Card for comparing the monitored amount of time to a predetermined reference time;

(d) means disposed within the PCMCIA Card for refusing to permit completion of the bus transaction if the monitored amount of time exceeds the predetermined reference time.

5. A system for protecting cryptographic processing and memory resources for postal franking machines, comprising an Application Specific Integrated

Circuit having (1) zeroizing circuitry, (2) read only memory, (3) random access memory, (4) a clock circuit, (5) non-volatile memory, (6) central cryptographic processor, (7) logic for addressing and data flow, (8) crypto key retention, (9) signature algorithm execution, (10) random number generator, (11) interrupt control and porting, (12) real time calendar clocking and watch-dog timer, (13) hash algorithm, (14) secure memory management unit, and (15) host interface.

6. A system for protecting cryptographic processing and memory resources for postal franking machines, comprising:

(a) an Application Specific Integrated Circuit having (1) zeroizing circuitry, (2) read only memory, (3) random access memory, (4) a clock circuit, (5) non-volatile memory, (6) central cryptographic processor, (7) logic for addressing and data flow, (8) crypto key retention, (9) signature algorithm execution, (10) random number generator, (11) interrupt control and porting, (12) real time calendar clocking and watch-dog timer, (13) hash algorithm, (14) secure memory management unit, and (15) host interface;

(b) said Application Specific Integrated Circuit being disposed within a Personal Computer Memory International Association card.

7. A method for protecting cryptographic processing and memory resources for postal franking machines, comprising locating the resources to be

protected within an Application Specific Integrated Circuit.

8. A system for protecting cryptographic processing and memory resources for postal franking machines, comprising (1) zeroizing circuitry, (2) read only memory, (3) random access memory, (4) a clock circuit, (5) non-volatile memory, (6) central cryptographic processor, (7) logic for addressing and data flow, (8) crypto key retention, (9) signature algorithm execution, (10) random number generator, (11) interrupt control and porting, (12) real time calendar clocking and watch-dog timer, (13) hash algorithm, (14) secure memory management unit, and (15) host interface, all disposed within a PCMCIA Card.

9. A method for protecting cryptographic processing and memory resources for postal franking machines, comprising locating the resources to be protected within a PCMCIA Card.

10. A method for protecting cryptographic processing and memory resources for postal franking machines disposed within PCMCIA Card, comprising:

(a) monitoring the amount of time a host controller is taking to complete a bus transaction;

(b) comparing the monitored amount of time to a predetermined reference time;

(c) refusing to permit completion of the bus transaction if the monitored amount of time exceeds the predetermined reference time.

11. A system for protecting cryptographic processing and memory resources for postal franking machines, comprising:

(a) an Application Specific Integrated Circuit having (1) zeroizing circuitry, (2) read only memory, (3) random access memory, (4) a clock circuit, (5) non-volatile memory, (6) central cryptographic processor, (7) logic for addressing and data flow, (8) crypto key retention, (9) signature algorithm execution, (10) random number generator, (11) interrupt control and porting, (12) real time calendar clocking and watch-dog timer, (13) hash algorithm, (14) secure memory management unit, and (15) host interface;

(b) an encryption engine disposed within the PCMCIA Card;

(c) means for obtaining encrypted code in portions to be processed by the encryption engine;

(d) random access memory disposed within the PCMCIA Card;

(e) means for placing decrypted output from the encryption engine into the random access memory.